Hindawi
Security and Communication Networks
Volume 2023, Article ID 3765934, 9 pages
https://doi.org/10.1155/2023/3765934

Research Article

Identity-Based Unidirectional Collusion-Resistant Proxy Re-Encryption from U-LWE

Nan Yang [1,2] **and Youliang Tian** [1]

[1]*State Key Laboratory of Public Big Data, College of Computer Science and Technology, Guizhou University, Guiyang 550025, China*
[2]*School of Mathematics and Statistics, Qiannan Normal University for Nationalities, Duyun, Guizhou 558000, China*

Correspondence should be addressed to Youliang Tian; youliangtian@163.com

Received 24 July 2022; Revised 19 October 2022; Accepted 1 November 2022; Published 3 January 2023

Academic Editor: Jie Cui

Identity-based proxy re-encryption (IB-PRE) converts the ciphertext encrypted under the delegator's identity to the one encrypted under the delegatee's identity through a semitrusted proxy without leaking delegator's private key and the underlying plaintext. At present, the security of most IB-PRE schemes relies on the hardness of the discrete logarithm solution or large integer decomposition and cannot resist attacks of the quantum algorithms. The majority of the IB-PRE schemes over lattice are secure only in the random oracle model. Aiming at such problems, the paper constructs a secure IB-PRE scheme over lattice in the standard model. In the scheme, the underlying encryption scheme proposed by Gentry et al. in EUROCRYPT 2010 is adopted to reduce the storage space of ciphertext. The proposed scheme is unidirectional collusion-resistant multihop and anonymous, and it is semantically secure against selective identity and chosen plaintext attack based on Decisional Learning With Errors with uniformly distributed errors (D-U-LWE) hard problem in the standard model.

1. Introduction

Proxy re-encryption (PRE) scheme was introduced by Blaze et al. [1] in 1998. In the PRE scheme, the delegator sends ciphertext encrypted by delegator's public key to the proxy with re-encryption key, and the proxy converts the original ciphertext into one under delegatee's public key using the re-encryption key. In the process, neither plaintext nor delegator's private key is leaked to delegatee or proxy. Identity-based proxy re-encryption scheme integrates the idea of identity-based encryption into PRE scheme, and in the IB-PRE scheme, the unique identity of user, such as telephone number and ID number, can be used for the public key of the user. Meanwhile, the Public Key Infrastructure (PKI) is not required without the generation, distribution, and management of the public key relative to the general PRE scheme. So the IB-PRE scheme is applied in a variety of scenarios [2–5].

1.1. Related Work. Since Blaze et al. first proposed and constructed the PRE scheme, the hardness of the PRE scheme is mainly based on the classical number theory hard problems or hard problems over lattice. The underlying classical number theory hard problems, such as large integer factorization hard problem and discrete logarithm hard problem, can be efficiently broken by the quantum algorithm [6] in the polynomial time. With the rapid progress of quantum algorithm technologies, constructing the lattice based PRE scheme to realize the quantum-resistant attack is very meaningful. The first lattice based PRE scheme was introduced by Xagawa [7] in his doctor of philosophy thesis, the scheme was bidirectional and not collusion-resistant attack. Aono et al. [8] proposed the key-private PRE scheme under LWE hard problem without leaking the identity of delegator and delegatee, whereas the scheme cannot resist the collusion attack of the proxy and delegatee, the scheme is CPA secure in the standard model and is CCA secure in the

random oracle model. Singh et al. [9] constructed the first lattice based anonymous IB-PRE scheme; however, the scheme is bidirectional in which if the proxy and the delegatee are collusive, the private key of the delegator is leaked easily. Whereafter, Singh et al. [10] designed a new re-encryption key to resolve the problem of collusion in the literature [8] and constructed a lattice based unidirectional and multihop IB-PRE scheme. In the same year, Singh et al. [11] introduced another new lattice based unidirectional and multihop IB-PRE scheme using the strong trapdoor method [12], the scheme was shown unable to resist collusion attack in the literature [13]. [9–11] are IND-sID-CPA secure in the random oracle model.

Jiang et al. [14] constructed the first lattice based multihop unidirectional PRE scheme using the underlying encryption scheme [15] with the IND-CPA security in the standard model, on the basis, a lattice based IB-PRE scheme was constructed with the IND-CPA security in the standard model, and also was multihop and unidirectional, whereas the detailed security proof was not given out. Wang et al. [16] indicated the re-encryption ciphertext had high decryption error rate in the literature [14], and subsequently presented a unidirectional collusion-resistant PRE scheme with the IND-CPA security in the standard model. Hou et al. [17] presented a multibit bidirectional IND-ID-CPA secure IB-PRE scheme. The hardness of the above lattice based schemes is based on the LWE hard problem or its variants. For the lack of unidirectionality or collusion-resistance, our focus is to present a unidirectional multihop and collusion-resistant IB-PRE scheme over lattice.

1.2. Contributions. The paper mainly constructs a novel IB-PRE scheme in the context of BGN-type cryptosystem [15] over lattice. To implement the scheme, some techniques are employed such as trapdoor generation algorithm [18] and Bonsai Trees algorithm [19]. In the setup phase, using trapdoor generation algorithm generates the public parameters pp and the master key $\mathbf{T}_{\mathbf{A}_0}$, i.e., a short basis of the random lattice $\wedge_q^{\perp}(\mathbf{A}_0)$ as the relevant trapdoor. The private key of the user is created by the Bonsai Trees algorithm that utilizes relatively "small" $(\mathbf{A}_0, \mathbf{T}_{\mathbf{A}_0})$ to obtain relatively "big" $(\mathbf{F}_{\mathbf{id}}, \mathbf{sk}_{\mathbf{id}})$. The plaintext μ is encrypted by user (delegator) id's public key $\mathbf{F}_{\mathbf{i}\ \mathbf{d}}$ to gain the second-level ciphertext $\mathbf{C}_{\mathbf{id}} = \mathbf{F}_{\mathbf{id}}^T\mathbf{s} + 2\mathbf{e}_1 + \mu\mathbf{b}_1 \bmod q$. In order to translate the second-level ciphertext $\mathbf{C}_{\mathbf{id}_i}$ to the first-level ciphertext $\mathbf{C}_{\mathbf{id}_j} = \mathbf{F}_{\mathbf{id}_j}^T\mathbf{s}_2 + 2\mathbf{e}_2 + \mu\mathbf{b}_2 \bmod q$, we constructed the re-encryption key $\mathbf{rk}_{\mathbf{id}_i \longrightarrow \mathbf{id}_j} = \mathbf{F}_{\mathbf{id}_j}^T\mathbf{L}_1 + \mathbf{R}_1\mathbf{sk}_{\mathbf{id}_i}^T \bmod q$ such that $\mathbf{C}_{\mathbf{id}_j} = \mathbf{rk}_{\mathbf{id}_i \longrightarrow \mathbf{id}_j}\mathbf{C}_{\mathbf{id}_i} + 2\mathbf{t}_1 \bmod q$, where $\mathbf{rk}_{\mathbf{id}_i \longrightarrow \mathbf{id}_j}$ is similar to U-LWE hard problem form.

2. Preliminaries

2.1. Notations. We exploit $\mathbb{Z}$ and $\mathbb{R}$ to denote the sets of integers and real numbers, respectively, and represent scalars by the lowercase letters, vectors by the lowercase bold letters, and matrixes by the uppercase bold letters. A vector can be represented in terms of column vector and a matrix can be denoted by the ordered column vectors, such as matrix $\mathbf{A} = \{\mathbf{a}_1, \ldots, \mathbf{a}_\mathbf{m}\}$. $\|\mathbf{x}\|$ denotes the $\mathbf{l}_2$-norm of the vector $\mathbf{x}$. The norm $\|\mathbf{A}\|$ of the matrix $\mathbf{A}$ is the $\max\{\|\mathbf{a}_\mathbf{i}\|\}$. $\mathbf{A}^T$ is used to denote the transpose of the matrix $\mathbf{A}$, the symbol $(\mathbf{A}|\mathbf{B})$ indicates that matrixes are connected horizontally to construct a new matrix.

The notation $\widetilde{\mathbf{a}}$ presents the Gram-Schmidt orthogonalization of the vector $\mathbf{a}$ and $\widetilde{\mathbf{A}}$ denotes the Gram-Schmidt orthogonalization of the matrix $\mathbf{A}$. The $\mathrm{poly}(\cdot)$ expresses an unspecified polynomial function, the function $\epsilon(n)$ presents a negligible function, i.e., $\epsilon(n) = (1/\mathrm{poly}(n))$, where n is an arbitrary positive integer.

2.2. Lattice

Definition 1. $\mathbf{a}_1, \ldots, \mathbf{a}_\mathbf{n} \in \mathbb{R}^m$ are linearly independent. The lattice is the set of all integer coefficient linear combination of $\mathbf{a}_1, \ldots, \mathbf{a}_\mathbf{n}$. The lattice $L(\mathbf{A}) = L(\mathbf{a}_1, \ldots, \mathbf{a}_\mathbf{n}) = \{\sum_{i=1}^n z_i\mathbf{a}_\mathbf{i} | \quad z_i \in \mathbb{Z},\ \mathbf{a}_\mathbf{i} \in \mathbb{R}^m\}$, where $\mathbf{a}_1, \ldots, \mathbf{a}_\mathbf{n}$ is the basis, n is the rank, and m is the dimension for the lattice. Generally, when $n = m$, the lattice is called full rank lattice. In the paper, we use a kind of special integer lattices called "q – ray" random lattices.

Definition 2. Set q as a prime number, $\mathbf{A} \in \mathbb{Z}_q^{n\times m}$, the random lattices are defined as follows:

$$\begin{aligned}\wedge_q^{\perp}(\mathbf{A}) &= \left\{\mathbf{z} \in \mathbb{Z}^m | \mathbf{Az} = \mathbf{0},\ \mathbf{A} \in \mathbb{Z}_q^{n\times m}\right\},\\ \wedge_q^{u}(\mathbf{A}) &= \left\{\mathbf{z} \in \mathbb{Z}^m | \mathbf{Az} = \mathbf{u}, \quad \mathbf{A} \in \mathbb{Z}_q^{n\times m},\ \mathbf{u} \in \mathbb{Z}_q^n\right\},\end{aligned} \tag{1}$$

where $\wedge_q^{\perp}(\mathbf{A})$ and $\wedge_q^{u}(\mathbf{A})$ are full rank integer lattices.

We introduce trapdoor generation algorithm. Using the algorithm, we can output a random matrix and a "short" basis of random lattice generated by the matrix. The matrix is used to construct a user's public key and the basis is an input of the private key extraction algorithm, which we construct to generate the user's private key in the scheme.

Lemma 1. *Trapdoor generation algorithm [18]. For the parameters n, $q = poly(n)$ and $m \geq 6n\log q$, there is a probabilistic polynomial time (PPT) algorithm $TrapGen(q, n, m)$, it generates pseudo-random matrix $\mathbf{A} \in \mathbb{Z}_q^{n\times m}$ and a "short" trapdoor basis $\mathbf{T}_\mathbf{A} \in \mathbb{Z}^{m\times m}$ for the lattice $\wedge_q^{\perp}(\mathbf{A})$, where the distribution of $\mathbf{A}$ is statistically close to uniform distribution over $\mathbb{Z}_q^{n\times m}$ and the length $\|\widetilde{\mathbf{T}}_\mathbf{A}\| \leq O(\sqrt{n\log q})$.*

Lemma 2. *Bonsai Trees algorithm [19]. The Bonsai Trees algorithm has four basic procedures: undirected growth, controlled growth, extending control, and randomizing control.*

Undirected growth. $\mathbf{A}$ is an arbitrary matrix in $\mathbb{Z}_q^{n\times m}$ and $\mathbf{A}' = (\mathbf{A}|\overline{\mathbf{A}}) \in \mathbb{Z}_q^{n\times m'}$ for some $m' > m$ is an arbitrary extension of A.

Controlled growth. It is actually trapdoor generation algorithm.

Extending control. $\mathbf{T} \in \mathbb{Z}^{m\times m}$ is an arbitrary basis of $\wedge_q^{\perp}(\mathbf{A})$, $\overline{\mathbf{A}} \in \mathbb{Z}_q^{n\times m'}$ is an arbitrary matrix. There exists a

deterministic polynomial time algorithm $\text{Ext Basis}(\mathbf{T}, (\mathbf{A}|\overline{\mathbf{A}}))$, which outputs a basis $\overline{\mathbf{T}}$ of $\wedge_q^{\perp}((\mathbf{A}|\overline{\mathbf{A}}))$, where $\|\widetilde{\mathbf{T}}\| = \|\overline{\mathbf{T}}\|$.

Randomizing control. Set parameters $s \in \mathbb{R}$ and $\mathbf{A} \in \mathbb{Z}_q^{n\times m}$, $\mathbf{T}$ is a basis of $\wedge_q^{\perp}(\mathbf{A})$ satisfying $s \geq \|\widetilde{\mathbf{T}}\|\omega(\sqrt{\log n})$, there exists a PPT algorithm $\text{Rand Basis}(\mathbf{T}, \mathbf{s})$, which generates a basis $\mathbf{T}'$ of $\wedge_q^{\perp}(\mathbf{A})$ with $\|\mathbf{T}'\| \leq s\sqrt{m}$. Moreover, for two arbitrary basis $\mathbf{T}_1$ and $\mathbf{T}_2$, where $s \geq \max\left\{\|\widetilde{\mathbf{T}}_1\|, \|\widetilde{\mathbf{T}}_2\|\right\}\omega(\sqrt{\log n})$, the outputs of $\text{Rand Basis}(\mathbf{T}_1, \mathbf{s})$ and $\text{Rand Basis}(\mathbf{T}_2, \mathbf{s})$ are statistically indistinguishable.

Regarding Lemma 2, in our scheme, the extending control procedure can extend a basis of the low-dimension lattice (i.e., $\wedge_q^{\perp}(\mathbf{A}_0)$) to the one of the high-dimension lattice (i.e., $\wedge_q^{\perp}(\mathbf{A}_{\mathbf{i}\,\mathbf{d}})$) with loss in quality. Using randomizing control procedure, the private key of a user is generated.

2.3. A Variant of Learning with Errors (LWE). The learning with errors was introduced by Regev [20]. Based on the LWE hard problem, cryptologists construct various cryptography schemes in the lattice cryptography, meanwhile, LWE hard problem generates a few variants, U-LWE is one of them.

Definition 3 ([21]). Give parameters n, sufficiently small real constant number $\epsilon \in (0, 1)$, modular integer $q = \text{poly}(n)$, dimension integer $m = \text{poly}(n) \geq 3n$, real number $r \geq 2n^{0.5+\epsilon}m$. If there is a PPT algorithm to successfully resolve LWE $(n, q, m, U[-r, r])$ with non-negligible probability in the polynomial time, then there exists an efficient quantum algorithm that can resolve the appropriate decisional the shortest vector problem (GAPSVP) and the shortest independent vectors problem (SIVP) to within $\widetilde{O}(n^{1+\epsilon}mq/r)$ in the worst case.

At the level of the parameters in the Definition 3, the decisional version of the U-LWE (D-U-LWE) problem is hard [21]. In our secure proof, the D-U-LWE hard problem is used for proving Game 2 and Game 3 indistinguishable.

2.4. Encoding with Full-Rank Differences. In our IB-PRE scheme, we utilize an identity encoding function, i.e., encoding with full-rank differences (FRD) [22], to translate the identity of a user to the matrix in the $\mathbb{Z}_q^{n\times 2m}$.

Definition 4. Encoding with full-rank differences.

Let function $H: \mathbb{Z}_q^n \longrightarrow \mathbb{Z}_q^{n\times n}$ satisfy the following conditions:

(1) For all distinct $\mathbf{x}_1, \mathbf{x}_2 \in \mathbb{Z}_q^n$, $H(\mathbf{x}_1) - H(\mathbf{x}_2) \in \mathbb{Z}_q^{n\times n}$ is full rank

(2) For zero vector $\mathbf{0} \in \mathbb{Z}_q^n$, $H(\mathbf{0}) = \mathbf{0} \in \mathbb{Z}_q^{n\times n}$

(3) The function H is efficiently and correctly computed in polynomial time

Note the function H is injective.

2.5. IB-PRE Scheme Model. The IB-PRE scheme contains the following six algorithms [23].

(1) Setup (n): Input secret parameter n and output the public parameters pp and the master secret key msk

(2) Extract (pp, id, msk): Input the public parameters pp, the master secret key msk, and the user's identity id, and output the private key $\mathbf{sk}_{\mathbf{i}\,\mathbf{d}}$ for the user id

(3) Enc $(pp, i\ d, \mu)$: Input the public parameters pp, the user's identity id, and message μ, and output a second-level ciphertext $\mathbf{C}_{\mathbf{id}}$ for the user id

(4) ReKeyGen (pp, sk_{id_j}, id_j): Input the public parameters pp, the private key $\mathbf{sk}_{\mathbf{id}_i}$ for the user id_i, and the user's identity id_j, and output the re-encryption key $\mathbf{rk}_{\mathbf{id}_i \longrightarrow \mathbf{id}_j}$ from id_i to id_j

(5) ReEnc $(pp, rk_{id_i \longrightarrow id_j}, C_{id_i})$: Input the public parameters pp, the re-encryption key $\mathbf{rk}_{\mathbf{id}_i \longrightarrow \mathbf{id}_j}$, and the second-level ciphertext $\mathbf{C}_{\mathbf{id}_i}$ of the user id_i, and output a first-level ciphertext $\mathbf{C}_{\mathbf{id}_j}$ of the user id_j

(6) Dec (pp, sk_{id}, C_{id}): Input the public parameters pp, the private key $\mathbf{sk}_{\mathbf{id}}$, and the ciphertext $\mathbf{C}_{\mathbf{id}}$ for the user $i\ d$, and output the plaintext μ

Correctness: If the scheme is correct, the following conditions must be met

$\text{Dec}\ (pp, sk_{id}, \mathbf{Enc}(pp, id, \mu)) = \mu$

$\text{Dec}\ (pp, sk_{id_j}, \mathbf{ReEnc}(pp, \mathbf{ReKeyGen}(pp, sk_{id_i}, id_j), \mathbf{Enc}(pp, id_i, \mu))) = \mu$

2.6. IB-PRE Security Model. The security of the IB-PRE scheme can be described with an interactive experiment (game) $\text{Exp}_{IB-\text{PRE},\mathscr{A}}^{\text{IND}-sI\ D-\text{CPA}}(n)$ between adversary $\mathscr{A}$ and challenger $\mathscr{B}$.

2.6.1. Setup Phase. Challenger $\mathscr{B}$ executes the setup algorithm with the secure parameter n and obtains the public parameters pp and master secret key msk, then sends the public parameters pp to adversary $\mathscr{A}$.

2.6.2. Phase 1. In the phase 1, adversary $\mathscr{A}$ wants to issue the following queries with no more than polynomial times, and challenger $\mathscr{B}$ answers the queries.

(1) Private key extract query: Adversary $\mathscr{A}$ inputs the identity id, and challenger $\mathscr{B}$ returns the private key $\mathbf{sk}_{\mathbf{i}\,\mathbf{d}} = \text{Extract}\ (pp, id, \text{msk})$, where $i\ d \neq id^*$ (id^* is the target identity), otherwise outputs $\perp$.

(2) Re-encryption key query: Adversary $\mathscr{A}$ inputs the identity pair (id_i, id_j), and challenger $\mathscr{B}$ returns the re-encryption key $\mathbf{rk}_{\mathbf{id}_i \longrightarrow \mathbf{id}_j} = \text{ReKeyGen}\ (pp, sk_{id_i}, id_j)$, where $id_i \neq id^*$, otherwise outputs $\perp$.

2.6.3. Challenge Phase. Adversary $\mathscr{A}$ transmits target identity id^* and messages $\mu_0 \neq \mu_1$ to challenger $\mathscr{B}$, then challenger $\mathscr{B}$ generates the challenge ciphertext

$C_{id^*} = \mathbf{Enc}(pp, id^*, \mu_i)$ for any randomly chosen $i \in \{0,1\}$ and returns C_{id^*} to adversary $\mathscr{A}$.

2.6.4. Phase 2. The phase 2 is same with phase 1.

2.6.5. Guess Phase. Challenger $\mathscr{A}$ outputs the guess result $\mu_{i'}$. If $\mu_{i'} = \mu_i$, challenger $\mathscr{A}$ wins and outputs 1, otherwise, challenger $\mathscr{A}$ fails and outputs 0.

Definition 5. The advantage of adversary $\mathscr{A}$ is defined as a function about the secure parameter n.

$$\mathrm{Adv}^{\mathrm{IND}-sID-\mathrm{CPA}}_{IB-\mathrm{PRE},\mathscr{A}}(n) = \left|\Pr\left[\mathrm{Exp}^{\mathrm{IND}-sI\,D-\mathrm{CPA}}_{IB-\mathrm{PRE},\mathscr{A}}(n) = 1\right] - (1/2)\right|. \tag{2}$$

For any polynomial time adversary $\mathscr{A}$, if there exists a negligible function $\epsilon(n)$ making $\mathrm{Adv}^{\mathrm{IND}-sID-\mathrm{CPA}}_{IB-\mathrm{PRE},\mathscr{A}}(n) \le \epsilon(n)$ true, the IB-PRE scheme is IND-sID-CPA secure.

The probability of an ordinary person, who does not interact with challenger $\mathscr{B}$, breaking the scheme is $(1/2)$. Adversary $\mathscr{A}$ may increase his knowledge by interacting with challenger $\mathscr{B}$ and obtain the ability to break the scheme. Therefore, the winning probability of adversary $\mathscr{A}$ is the sum of advantage probability and $(1/2)$. In Definition 5, when the absolute value of adversary $\mathscr{A}$'s winning probability minus $(1/2)$ is negligible, adversary $\mathscr{A}$'s advantage probability is negligible, and it means that adversary $\mathscr{A}$ is incapable to break the scheme, so the scheme is safe.

3. Our Scheme

In the section, we employ Gentry et al.'s scheme [15] to design a unidirectional collusion-resistant and multihop IB-PRE scheme. The process of the construction is as follows:

3.1. Construction

Setup (n)

Input secret parameter $n \in \mathbb{Z}$, $q = \mathrm{poly}(n)$ is an odd prime number, and $m = O(n \log q) = O(n \log n)$.

(1) Use trapdoor generation algorithm TrapGen (q, n, m) to generate random matrix $\mathbf{A}_0 \in \mathbb{Z}_q^{n\times m}$ and a "short" trapdoor basis $\mathbf{T}_{\mathbf{A}_0} \in \mathbb{Z}^{m\times m}$, where the distribution of $\mathbf{A}_0$ is statistically close to the uniform distribution over $\mathbb{Z}_q^{n\times m}$ and the length $\|\widetilde{\mathbf{T}}_{\mathbf{A}_0}\| \le O(\sqrt{n \log q})$.
(2) Select uniformly two matrixes $\mathbf{A}_1, \mathbf{B} \in \mathbb{Z}_q^{n\times m}$ at random. Set real number $\sigma \ge \|\widetilde{\mathbf{T}}_{\mathbf{A}_0}\|\omega(\sqrt{\log n})$.
(3) Set H as an identity encoding function.

Output public parameters $pp = \{\mathbf{A}_0, \mathbf{A}_1, \mathbf{B}, H, \sigma\}$ and master secret key $msk = \mathbf{T}_{\mathbf{A}_0}$.

Extract (pp, id, msk)

Input public parameters pp, user's identity $\mathbf{id} \in \mathbb{Z}_q^n$, and master secret key $\mathrm{msk} = \mathbf{T}_{\mathbf{A}_0}$.

(1) Encode the user's identity $\mathbf{id}$ as $\mathbf{F_{i\,d}} = (\mathbf{A}_0|\mathbf{A}_1 + H(\mathbf{i\ d})\mathbf{B})$.
(2) Compute user $\mathbf{id}$'s private key $\mathbf{sk_{id}}$ using Bonsai Trees algorithm. $\mathbf{sk_{id}} = \mathrm{Rand\,Basis}(\mathrm{Ext\,Basis}(\mathbf{T}_{\mathbf{A}_0}, \mathbf{F_{i\,d}}), \sigma)$ is a "short" basis of $\wedge_q^{\perp}(\mathbf{F_{id}})$ satisfying $\mathbf{F}_{id}\mathbf{sk_{i\,d}} = 0$, $\mathbf{sk_{id}} \in \mathbb{Z}^{2m\times 2m}$, and $\|\mathbf{sk_{id}}\| \le \sigma\sqrt{2m}$.

Output user's private key $\mathbf{sk_{id}}$.

Enc $(pp, i\ d, \mu)$

Input public parameters pp, user's identity $\mathbf{id}$, and message $\mu \in \{0,1\}$.

(1) Encode identity $\mathbf{id}$ as $\mathbf{F_{i\,d}} = (\mathbf{A}_0|\mathbf{A}_1 + H(\mathbf{id})\mathbf{B})$.
(2) Choose a uniformly random vector $\mathbf{e}_1 \in [-r, r]^{2m}$ and uniformly random nonzero vector $\mathbf{s} \in \mathbb{Z}_q^n$, set $\mathbf{b}_1 = \{1, 0, \ldots, 0\}^{2m}$.
(3) Set $\mathbf{C_{i\,d}} = \mathbf{F}_{\mathbf{i\,d}}^T\mathbf{s} + 2\mathbf{e}_1 + \mu\mathbf{b}_1 \bmod q$.

Output the second-level ciphertext $\mathbf{C_{id}}$.

ReKeyGen (pp, sk_{id_i}, id_j)

Input public parameters pp, user $\mathbf{id_i}$'s private key $\mathbf{sk_{id_i}}$, and encode user $\mathbf{id_j}$ to obtain the public key $\mathbf{F_{id_j}} = (\mathbf{A}_0|\mathbf{A}_1 + H(\mathbf{id_j})\mathbf{B})$.

Choose a uniformly random nonzero matrix $\mathbf{R}_1 \in \{-1, 1\}^{2m\times 2m}$.

Choose a uniformly random nonzero matrix $\mathbf{L}_1 \in \mathbb{Z}_q^{n\times 2m}$.

Output the re-encryption key $\mathbf{rk_{id_i \longrightarrow id_j}} = \mathbf{F}_{\mathbf{id_i}}^T\mathbf{L}_1 + \mathbf{R}_1\mathbf{sk}_{\mathbf{id_i}}^T \bmod q$
$= \mathbf{R}_1\mathbf{sk}_{\mathbf{id_i}}^T + \mathbf{F}_{\mathbf{id_j}}^T\mathbf{L}_1 \bmod q$.

ReEnc $(pp, rk_{id_i \longrightarrow id_j}, C_{id_i})$

Input public parameters pp, the re-encryption key $\mathbf{rk_{id_i \longrightarrow id_j}}$ from $\mathbf{id_i}$ to $\mathbf{id_j}$, and user $\mathbf{id_i}$'s ciphertext $\mathbf{C_{id_i}}$, and output user $\mathbf{id_j}$'s ciphertext $\mathbf{C_{id_j}}$.

$\mathbf{C_{id_j}} = \mathbf{rk_{id_i \longrightarrow id_j}}\mathbf{C_{id_i}} + 2\mathbf{t}_1 \bmod q$, where $\mathbf{t}_1 \in [-r, r]^{2m}$ is chosen uniformly at random.

Dec (pp, sk_{id}, C_{id})

Input public parameters pp, user's private key $\mathbf{sk_{id}}$, and the ciphertext $\mathbf{C_{id}}$.

Output plaintext μ. Compute $\mathbf{m} = (\mathbf{sk}_{\mathbf{id}}^T)^{-1}(\mathbf{sk}_{\mathbf{id}}^T\mathbf{C_{id}} \bmod q) \bmod 2$. If $\mathbf{m} = (0, \ldots, 0)$, output $\mu = 0$, otherwise output $\mu = 1$.

3.2. Parameters and Correctness. To ensure the correctness of the IB-PRE scheme, the parameters should content the following requirements:

(1) According to the trapdoor generation algorithm, the conditions of D-U-LWE hard problem [21] and the left hash lemma [22] require $m \ge 6n \log q$
(2) In the private key extraction algorithm, in order to correctly generate the user's private key, the algorithm uses the randomizing control procedure, satisfying $\sigma \ge \|\widetilde{\mathbf{T}}_{\mathbf{A}_0}\|\omega(\sqrt{\log n})$
(3) To make the D-U-LWE problem hard, the parameters r should satisfy $r \ge 2n^{0.5+\epsilon}m$, where real number $\epsilon > 0$

(4) In the algorithm Dec $(\cdot)$, we can achieve the decryption correctness of the second-level ciphertext by making sure the following inequalities are correct:
$\|\mathbf{sk}_{\mathbf{i}\,\mathbf{d}}^T \mathbf{e}_1\| \le r\sigma\sqrt{2m}\sqrt{m} = \sqrt{2}r\sigma m < (q/4)$.
$\|\mu\mathbf{sk}_{\mathbf{id}}^T \mathbf{b}_1\| \le \sigma\sqrt{2m} < (q/2)$
Therefore, $\sqrt{2}r\sigma m < (q/4)$, namely, $q > 4\sqrt{2}r\sigma m$.

(5) In the algorithm Dec $(\cdot)$, we can achieve the decryption correctness of the first-level ciphertext by making sure the following inequalities are correct:
$\|\mathbf{R}_1\| \le 12\sqrt{4m} = 24\sqrt{m}$ [22]
$\|\mathbf{sk}_{\mathbf{id}_j}^T \mathbf{R}_1 \mathbf{sk}_{\mathbf{id}_i}^T \mathbf{e}_1\| \le 48\sqrt{2}m^2\sigma^2 r < (q/4)$
$\|\mu\mathbf{sk}_{\mathbf{id}_j}^T \mathbf{R}_1 \mathbf{sk}_{\mathbf{id}_i}^T \mathbf{b}_1\| \le 48m^{3/2}\sigma^2 < (q/4)$
$\|\mathbf{sk}_{\mathbf{id}_j}^T \mathbf{t}_1\| < 2m\sigma r < (q/8)$

Therefore, $48\sqrt{2}m^2\sigma^2 r < (q/4)$, namely, $q > 192\sqrt{2}m^2\sigma^2 r$.

According to the above five constraints in the IB-PRE scheme, we choose parameters as follows: $m = 6n\lceil \log q \rceil$, $\sigma = O(\sqrt{n \log q})\omega(\sqrt{\log n})$, $q = O(m^2\sigma^2 r)$, and $r = 2n^{0.5+\epsilon}m$.

For the second-level ciphertext $\mathbf{C}_{\mathbf{id}}$, the correctness of the decryption is shown as follows:

$$\begin{aligned}\mathbf{sk}_{\mathbf{id}}^T \mathbf{C}_{\mathbf{id}} \bmod q &= \mathbf{sk}_{\mathbf{id}}^T\left(\mathbf{F}_{\mathbf{id}}^T \mathbf{s} + 2\mathbf{e}_1 + \mu\mathbf{b}_1\right) \bmod q \\ &= \mathbf{sk}_{\mathbf{id}}^T\left(2\mathbf{e}_1 + \mu\mathbf{b}_1\right) \bmod q = 2\mathbf{sk}_{\mathbf{id}}^T \mathbf{e}_1 + \mu\mathbf{sk}_{\mathbf{id}}^T \mathbf{b}_1 \bmod q.\end{aligned} \tag{3}$$

According to aforementioned the forth constraint, we can obtain $\mathbf{sk}_{\mathbf{id}}^T \mathbf{C}_{\mathbf{id}} \bmod q = 2\mathbf{sk}_{\mathbf{id}}^T \mathbf{e}_1 + \mu\mathbf{sk}_{\mathbf{id}}^T \mathbf{b}_1$.

$$\begin{aligned}\left(\mathbf{sk}_{\mathbf{id}}^T\right)^{-1}\left(\mathbf{sk}_{\mathbf{id}}^T \mathbf{C}_{\mathbf{id}} \bmod q\right) \bmod 2 &= \left(\mathbf{sk}_{\mathbf{id}}^T\right)^{-1}\left(2\mathbf{sk}_{\mathbf{id}}^T \mathbf{e}_1 + \mu\mathbf{sk}_{\mathbf{id}}^T \mathbf{b}_1\right) \bmod 2 \\ &= 2\mathbf{e}_1 + \mu\mathbf{b}_1 \bmod 2 = \mu\mathbf{b}_1 \bmod 2 = \mu\mathbf{b}_1.\end{aligned} \tag{4}$$

If $\mu\mathbf{b}_1 = 0$, then $\mu = 0$, otherwise $\mu = 1$.

For the first-level ciphertext $\mathbf{C}_{\mathbf{id}_j}$, the correctness of the decryption is shown as follows:

$$\begin{aligned}\mathbf{C}_{\mathbf{id}_j} = \mathbf{rk}_{\mathbf{id}_i \longrightarrow \mathbf{id}_j} \mathbf{C}_{\mathbf{id}_i} + 2\mathbf{t}_1 \bmod q &= \left(\mathbf{R}_1 \mathbf{sk}_{\mathbf{id}_i}^T + \mathbf{F}_{\mathbf{id}_j}^T \mathbf{L}_1\right)\left(\mathbf{F}_{\mathbf{id}_i}^T \mathbf{s} + 2\mathbf{e}_1 + \mu\mathbf{b}_1\right) + 2\mathbf{t}_1 \bmod q \\ &= \mathbf{R}_1 \mathbf{sk}_{\mathbf{id}_i}^T\left(2\mathbf{e}_1 + \mu\mathbf{b}_1\right) + \mathbf{F}_{\mathbf{id}_j}^T \mathbf{L}_1\left(\mathbf{F}_{\mathbf{id}_i}^T \mathbf{s} + 2\mathbf{e}_1 + \mu\mathbf{b}_1\right) + 2\mathbf{t}_1 \bmod q \\ &= \mathbf{F}_{\mathbf{id}_j}^T \mathbf{L}_1 \mathbf{F}_{\mathbf{id}_i}^T \mathbf{s} + 2\left(\mathbf{rk}_{\mathbf{id}_i \longrightarrow \mathbf{id}_j} \mathbf{e}_1 + \mathbf{t}_1\right) + \mu\mathbf{rk}_{\mathbf{id}_i \longrightarrow \mathbf{id}_j} \mathbf{b}_1 \bmod q.\end{aligned} \tag{5}$$

Let $\mathbf{s}_2 = \mathbf{L}_1 \mathbf{F}_{\mathbf{id}_i}^T \mathbf{s}$, $\mathbf{e}_2 = \mathbf{rk}_{\mathbf{id}_i \longrightarrow \mathbf{id}_j} \mathbf{e}_1 + \mathbf{t}_1$, $\mathbf{b}_2 = \mathbf{rk}_{\mathbf{id}_i \longrightarrow \mathbf{id}_j} \mathbf{b}_1$, then $\mathbf{C}_{\mathbf{id}_j} = \mathbf{F}_{\mathbf{id}_j}^T \mathbf{s}_2 + 2\mathbf{e}_2 + \mu\mathbf{b}_2$.

$$\begin{aligned}\mathbf{sk}_{\mathbf{id}_j}^T \mathbf{C}_{\mathbf{id}_j} \bmod q &= \mathbf{sk}_{\mathbf{id}_j}^T\left(\mathbf{F}_{\mathbf{id}_j}^T \mathbf{s}_2 + 2\mathbf{e}_2 + \mu\mathbf{b}_2\right) \bmod q \\ &= \mathbf{sk}_{\mathbf{id}_j}^T\left(\mathbf{R}_1 \mathbf{sk}_{\mathbf{id}_i}^T\left(2\mathbf{e}_1 + \mu\mathbf{b}_1\right)\right) + 2\mathbf{sk}_{\mathbf{id}_j}^T \mathbf{t}_1 \bmod q \\ &= 2\mathbf{sk}_{\mathbf{id}_j}^T \mathbf{R}_1 \mathbf{sk}_{\mathbf{id}_i}^T \mathbf{e}_1 + \mu\mathbf{sk}_{\mathbf{id}_j}^T \mathbf{R}_1 \mathbf{sk}_{\mathbf{id}_i}^T \mathbf{b}_1 + 2\mathbf{sk}_{\mathbf{id}_j}^T \mathbf{t}_1 \bmod q.\end{aligned} \tag{6}$$

According to aforementioned fifth constraint, we can obtain the following constraint:

$$\begin{aligned}&\mathbf{sk}_{\mathbf{id}_j}^T \mathbf{C}_{\mathbf{id}_j} \bmod q \\ &\quad = 2\mathbf{sk}_{\mathbf{id}_j}^T \mathbf{R}_1 \mathbf{sk}_{\mathbf{id}_i}^T \mathbf{e}_1 + \mu\mathbf{sk}_{\mathbf{id}_j}^T \mathbf{R}_1 \mathbf{sk}_{\mathbf{id}_i}^T \mathbf{b}_1 + 2\mathbf{sk}_{\mathbf{id}_j}^T \mathbf{t}_1.\end{aligned} \tag{7}$$

We compute,

$$\mathbf{m} = \left(\mathbf{sk}_{\mathbf{id}_j}^T\right)^{-1}\left(\mathbf{sk}_{\mathbf{id}_j}^T \mathbf{C}_{\mathbf{id}_j} \bmod q\right) \bmod 2 = \mu\mathbf{R}_1 \mathbf{sk}_{\mathbf{id}_i}^T \mathbf{b}_1 \bmod 2. \tag{8}$$

If $\mathbf{m} = \mu\mathbf{R}_1 \mathbf{sk}_{\mathbf{id}_i}^T \mathbf{b}_1 \bmod 2 = 0$, output 0, otherwise output 1.

Because of the left hash lemma, $\mathbf{R}_1 \mathbf{sk}_{\mathbf{id}_i}^T$ is uniform and random, the probability of the $\mathbf{R}_1 \mathbf{sk}_{\mathbf{id}_i}^T \mathbf{b}_1 \bmod 2 = 0$ is $(1/4^m)$. The error probability of the first-level decryption is $(1/4^m)$ and is negligible.

3.3. Security Analysis

Theorem 1. *Let q, m, σ, and r be as in the aforementioned qualifications, then the IB-PRE scheme described above is IND-sID-CPA secure, assuming the D-U-LWE problem is hard.*

Proof. In order to show the scheme is secure, we use a sequence of games to prove the advantage of adversary $\mathscr{A}$ is negligible.

In the sequence of games, Game_0 is identical with original IB-PRE scheme, and the advantage of adversary $\mathscr{A}$ is zero in Game_3. Finally, we demonstrate that adversary $\mathscr{A}$ cannot distinguish four games and win in Game_0 with negligible advantage, while the D-U-LWE hard problem is used for proving Game_2 and Game_3 indistinguishable. □

3.3.1. $Game_0$. This is the original IB-PRE scheme. Adversary $\mathscr{A}$ creates the challenge identity $\mathbf{id}^*$ before the setup phase. Challenger $\mathscr{B}$ gains the private key of user $\mathbf{i\,d}\,(\neq \mathbf{id}^*)$ and re-encryption keys from $\mathbf{i\,d}$ to other users, with algorithms Extract $(\cdot)$ and ReKeyGen $(\cdot)$, separately.

3.3.2. $Game_1$. The difference between $Game_0$ and $Game_1$ is only the generation type of the public matrix $\mathbf{A}_1$. In Game_1, challenger $\mathscr{B}$ produces $\mathbf{A}_1$ by calculating $\mathbf{A}_1 = \mathbf{A}_0\mathbf{R}^* - \mathbf{H}(\mathbf{id}^*)\mathbf{B}$, where $\mathbf{R}^* \in \{-1, 1\}^{m\times m}$ denotes a uniformly random matrix. The rest of the part of Game_1 is same with Game_0.

In Game_1, according to the left hash lemma, the distribution of $\mathbf{A}_0\mathbf{R}^*$ is statistically close to the uniform distribution over $\mathbb{Z}_{\mathbf{q}}^{n\times m}$, hence, the distribution of $\mathbf{A}_1$ is statistically close to the uniform distribution over $\mathbb{Z}_{\mathbf{q}}^{n\times m}$. Therefore, in the view of adversary $\mathscr{A}$, $\mathbf{A}_1$ in $Game_0$ and Game_1 are indistinguishable; furthermore, Game_0 and Game_1 are indistinguishable as well.

3.3.3. $Game_2$. In Game_2, we change the way of the generation about public matrixes $\mathbf{A}_0$ and $\mathbf{B}$, where $\mathbf{A}_0$ is uniformly and randomly sampled from $\mathbb{Z}_q^{n\times m}$ and $\mathbf{B}$ is generated by the trapdoor generation algorithm TrapGen $(\cdot)$ with a "short" trapdoor basis $\mathbf{T_B}$ of $\Lambda_q^{\perp}(\mathbf{B})$; hence, $\mathbf{B}$ is statistically close to uniformly random distribution over $\mathbb{Z}^{n\times m}$. $\mathbf{A}_0$ and $\mathbf{B}$ in Game_1 and Game_2 are indistinguishable severally. The choice of $\mathbf{A}_1$ is identical as in Game_1.

Challenger $\mathscr{B}$ responds to the private key query of the user $\mathbf{id}\,(\neq \mathbf{id}^*)$ as follows:

(1) Encode $\mathbf{id}$ as $\mathbf{F_{id}} = (\mathbf{A}_0|\mathbf{A}_1 + \mathbf{H}(\mathbf{id})\mathbf{B}) = (\mathbf{A}_0|\mathbf{A}_0\mathbf{R}^* + (\mathbf{H}(\mathbf{id}) - \mathbf{H}(\mathbf{id}^*))\mathbf{B})$.

(2) Generate a basis $\mathbf{T}_{\mathbf{F_{id}}}$ of $\Lambda_q^{\perp}(\mathbf{F_{id}})$ using the algorithm SampleRight $(\cdot)$ [22] in which the syndrome is zero vector.

(3) Generate $\mathbf{id}$'s private key $\mathbf{sk_{id}}$ using the randomizing control procedure in the Bonsai Trees algorithm, where $\mathbf{sk_{id}} = \text{Rand Basis}(\mathbf{T}_{\mathbf{F_{id}}}, \sigma)$ is a "short" basis of $\Lambda_q^{\perp}(\mathbf{F_{id}})$ satisfying $\mathbf{F}_{id}\mathbf{sk_{id}} = \mathbf{0}$. Hence, the distribution of $\mathbf{sk_{id}}$ is statistically indistinguishable with the one of $\mathbf{sk_{id}}$ in Game_1.

When adversary $\mathscr{A}$ proposes the query for re-encryption key $\mathbf{rk}_{\mathbf{id_i}\longrightarrow\mathbf{id_j}}$, challenger $\mathscr{B}$ replies $\mathscr{A}$ with $\mathbf{rk}_{\mathbf{id_i}\longrightarrow\mathbf{id_j}} = \mathbf{R}_1\mathbf{sk}_{\mathbf{id}}^T + \mathbf{F}_{\mathbf{id_j}}^T\mathbf{L}_1$. Therefore, in the view of adversary $\mathscr{A}$, $\mathbf{rk}_{\mathbf{id_i}\longrightarrow\mathbf{id_j}}$ in Game_1 and Game_2 are indistinguishable, Game_1 and Game_2 are indistinguishable as well.

3.3.4. $Game_3$. Challenger $\mathscr{B}$ uniformly chooses ciphertext $\mathbf{C}_{\mathbf{id}^*} \in \mathbb{Z}_q^{2m}$ at random and returns $\mathbf{C}_{\mathbf{id}^*}$ to adversary $\mathscr{A}$. Because of the randomness and uniformity of the ciphertext, the advantage of adversary $\mathscr{A}$ is zero in the game.

Lemma 3. *Under the D-U-LWE hard problem, $Game_2$ and $Game_3$ are indistinguishable in the view of adversary $\mathscr{A}$.*

Proof. Assume that adversary $\mathscr{A}$ can distinguish the Game_2 and Game_3 with non-negligible advantage ε, we can construct an algorithm (simulator) $\mathscr{B}$ to solve the D-U-LWE hard problem.

Algorithm $\mathscr{B}$ receives a random instance $(\mathbf{F}, \mathbf{Y}) \in \mathbb{Z}_q^{n\times 2m} \times \mathbb{Z}_q^{2m}$, where $(\mathbf{F}, \mathbf{Y})$ is either $(\mathbf{F}_{\mathbf{id}^*}, \mathbf{F}_{\mathbf{id}^*}^T\mathbf{s} + \mathbf{e}_1 \bmod q)$ or a uniformly random element over $\mathbb{Z}_q^{n\times 2m} \times \mathbb{Z}_q^{2m}$.

Next, algorithm $\mathscr{B}$ receives messages $\mu_0, \mu_1 \in \{0, 1\}$, and challenge identity $\mathbf{id}^*$. Algorithm $\mathscr{B}$ randomly selects $i \in \{0, 1\}$ and returns the challenge ciphertext $2\mathbf{Y} + \mu_i\mathbf{b}_1 \bmod q$ to adversary $\mathscr{A}$. If adversary $\mathscr{A}$ correctly guesses i, outputs 1, otherwise outputs 0.

On the one hand, if $\mathbf{Y}$ is uniformly chosen at random, regardless of the choice of i, the challenge ciphertext is uniformly random, therefore, algorithm $\mathscr{B}$ outputs 1 with probability $(1/2)$ at most.

On the other hand, if $\mathbf{Y} = \mathbf{F}_{\mathbf{id}^*}^{\mathbf{T}}\mathbf{s} + \mathbf{e}_1 \bmod q$, the challenge ciphertext is $2\mathbf{Y} + \mu_{\mathbf{i}}\mathbf{b}_1 = \mathbf{F}_{\mathbf{id}^*}^T\mathbf{s}' + 2\mathbf{e}_1 + \mu_i\mathbf{b}_1 \bmod q$, where $\mathbf{s}' = 2\mathbf{s} \bmod q$ is uniformly random (because of $(q, 2) = 1$). At this time, adversary $\mathscr{A}$ correctly guesses the i with probability $(1/2) + \varepsilon$.

The probability of the algorithm $\mathscr{B}$ receiving a random instance $(\mathbf{F}, \mathbf{Y})$ is $(1/2)$. According to the assumption, adversary $\mathscr{A}$ correctly guesses i with the probability $(1/2)(1/2 + 1/2 + \varepsilon) = (1 + \varepsilon)/2$, this means that algorithm $\mathscr{B}$ outputs 1 with the probability $(1 + \varepsilon)/2$, and therefore breaks the D-U-LWE hard problem with the advantage $(\varepsilon/2)$, and it is non-negligible.

Because D-U-LWE problem is the hard problem, the advantage of algorithm $\mathscr{B}$ in breaking the D-U-LWE hard problem is negligible. That is contradictory, so adversary $\mathscr{A}$'s advantage in distinguishing Game_2 with Game_3 is negligible.

In conclusion, because Game_0 and Game_1 are indistinguishable for adversary $\mathscr{A}$, Game_1 and Game_2, and Game_2 and Game_3 are also the same, meanwhile, adversary $\mathscr{A}$'s advantage is zero in the Game_3, so the advantage of the adversary $\mathscr{A}$ is negligible in the IB-PRE scheme described above and the IB-PRE scheme is IND-sID-CPA secure in the standard model. □

Table 1: Comparison to the related works.

Cryptosystem	Private key size	Unidirectionality	Collusion-resistance	Multihop	Security model
[9]	O $(ms \log q)$	No	No	Yes	Random oracle model
[11]	O $(ms(1+k)\log q)$	Yes	No	No	Random oracle model
[14]	O $(m^2 \log q)$	Yes	Yes	Yes	Standard model
[16]	O $(mn \log q)$	No	No	Yes	Standard model
Our scheme	O $(mn \log q)$	Yes	Yes	Yes	Standard model

4. Property

The IB-PRE scheme has desired properties as follows:

4.1. Multihop. An IB-PRE scheme is multihop if ciphertext is re-encrypted multiple times, on the contrary, it is single-hop. Multihop supports multiple encryption of ciphertext, that is, it allows delegating decryption right among multiple users. Single-hop only allows delegating decryption right between two users. In the multiuser scenario, multihop property is required generally.

For simplicity, we present the identities of the users as $1, 2, \ldots, v\,(v > 1)$, where the users participate in the process of re-encryption. According to the IB-PRE scheme, we can obtain the re-encryption procedure, which is performed from user 1 to user $l\,(1 < l \le v)$ as follows:

$$\begin{aligned}
\mathbf{C}_1 &= \mathbf{F}_1^T \mathbf{s}_1 + 2\mathbf{e}_1 + \mu \mathbf{b}_1 \bmod q,\\
\mathbf{C}_2 &= \mathbf{rk}_{1\longrightarrow 2}\mathbf{C}_1 + 2\mathbf{t}_2 \bmod q = \mathbf{F}_2^T \mathbf{L}_1 \mathbf{F}_1^T \mathbf{s}_1 + 2\left(\mathbf{rk}_{1\longrightarrow 2}\mathbf{e}_1 + \mathbf{t}_2\right) + \mu \mathbf{rk}_{1\longrightarrow 2}\mathbf{b}_1 \bmod q,\\
\mathbf{C}_3 &= \mathbf{rk}_{2\longrightarrow 3}\mathbf{C}_2 + 2\mathbf{t}_3 \bmod q = \mathbf{F}_3^T \mathbf{L}_2 \mathbf{F}_2^T \mathbf{L}_1 \mathbf{F}_1^T \mathbf{s}_1 + 2\mathbf{rk}_{1\longrightarrow 2}\mathbf{rk}_{2\longrightarrow 3}\mathbf{e}_1 + 2\mathbf{rk}_{2\longrightarrow 3}\mathbf{t}_2\\
&\quad + 2\mathbf{t}_3 + \mu \mathbf{rk}_{1\longrightarrow 2}\mathbf{rk}_{2\longrightarrow 3}\mathbf{b}_1 \bmod q.
\end{aligned} \tag{9}$$

$$\begin{aligned}
&\vdots\\
&\mathbf{C}_\mathbf{l} = \mathbf{rk}_{\mathbf{l}-1\longrightarrow \mathbf{l}}\mathbf{C}_{\mathbf{l}-1} + 2\mathbf{t}_\mathbf{l} \bmod q\\
&\quad = \mathbf{F}_\mathbf{l}^T \left(\prod_{i=1}^{l-1} \mathbf{L}_\mathbf{i} \mathbf{F}_\mathbf{i}^T\right)\mathbf{s}_1 + 2\left[\sum_{j=2}^{l}\left(\prod_{i=j}^{l} \mathbf{rk}_{\mathbf{i}-1\longrightarrow \mathbf{i}}\right)\mathbf{t}_{\mathbf{j}-1} + \mathbf{t}_\mathbf{l}\right] + \mu\left(\prod_{i=2}^{l} \mathbf{rk}_{\mathbf{i}-1\longrightarrow \mathbf{i}}\right)\mathbf{b}_1 \bmod q = \mathbf{F}_\mathbf{l}^T \mathbf{s}_\mathbf{l} + 2\mathbf{e}_\mathbf{l} + \mu \mathbf{b}_\mathbf{l} \bmod q,
\end{aligned} \tag{10}$$

where $\mathbf{s}_\mathbf{l} = (\prod_{i=1}^{l-1} \mathbf{L}_\mathbf{i}\mathbf{F}_\mathbf{i}^T)\mathbf{s}_1$, $\mathbf{e}_1 = \mathbf{t}_1$, $\mathbf{e}_\mathbf{l} = \sum_{j=2}^{l}(\prod_{i=j}^{l} \mathbf{rk}_{\mathbf{i}-1\longrightarrow \mathbf{i}})\mathbf{t}_{\mathbf{j}-1} + \mathbf{t}_\mathbf{l}$, and $\mathbf{b}_\mathbf{l} = (\prod_{i=2}^{l} \mathbf{rk}_{\mathbf{i}-1\longrightarrow \mathbf{i}})\mathbf{b}_1$.

According to the mathematical induction, the above equation is correct. If each entry of the $2\mathbf{sk}_\mathbf{l}^T\mathbf{e}_\mathbf{l} + \mu\mathbf{sk}_\mathbf{l}^T\mathbf{b}_\mathbf{l}$ is less than q, the error probability of the decryption is $(1/4^m)$ and is negligible.

4.2. Unidirectionality. The property is related to the direction of delegation, and is portrayed by re-encryption key. Unidirectionality means the decryption rights are only authorized from delegator to delegatee, otherwise, the scheme is bidirectional. The bidirectional scheme requires delegator and delegatee are confident in each other, however, the situation is not common in most applications. Because re-encryption key $\mathbf{rk}_{\mathbf{id}_\mathbf{i} \longrightarrow \mathbf{id}_\mathbf{j}} = \mathbf{F}_{\mathbf{id}_\mathbf{j}}^T \mathbf{L}_1 + \mathbf{R}_1 \mathbf{sk}_{\mathbf{id}_\mathbf{i}}^T \bmod q$ is U-LWE form, $\mathbf{rk}_{\mathbf{id}_\mathbf{i} \longrightarrow \mathbf{id}_\mathbf{j}}$ is uniformly pseudo-random in the view of the proxy and the delegatee under the D-U-LWE assumption, and the proxy and the delegatee are not able to construct a re-encryption key from delegatee to delegator, and our scheme is unidirectional.

4.3. Collusion-Resistance. The property is that the plaintext or private key of delegator cannot be leaked against collusion attack made by the delegatee and the proxy, that is, the private key of the delegator cannot be obtained from the re-encryption key and the delegatee's private key. Because re-encryption key $\mathbf{rk}_{\mathbf{id}_\mathbf{i} \longrightarrow \mathbf{id}_\mathbf{j}}$ is pseudo-random under the D-U-LWE assumption, the proxy and the delegatee cannot obtain the private key of delegator with collusion.

4.4. Noninteractivity. The property is that the delegator is capable of yielding a re-encryption key using the private key of delegator and the public key of delegatee without the participation of delegatee. In most cases, interactivity is not a desired property, because it can lead to communication overheads and may even be attacked by collusion of the proxy and delegatee. From the generation process of $\mathbf{rk}_{\mathbf{id}_\mathbf{i} \longrightarrow \mathbf{id}_\mathbf{j}}$, we can find that re-encryption key can be implemented alone by the delegator without interaction with the delegatee or other trusted the third parties.

4.5. Anonymousness. Anonymousness is that the second-level ciphertext and the first-level ciphertext do not reveal identity messages about the delegator and delegatee. This property protects the privacy of users. The distributions of the second-level ciphertext and the first-level ciphertext meet U-LWE distribution, which is pseudo-random, in our

scheme, so they do not leak any identity message about the delegator and delegatee.

5. Comparison

We compare our IB-PRE scheme with the other relevant IB-PRE schemes over lattice in terms of private key size, unidirectionality, collusion-resistance, multihop, and security model. The result is shown in Table 1, where s is the length of message and $k = \lceil \log q \rceil$.

6. Conclusion

In the paper, we constructed a unidirectional and multihop IB-PRE scheme with underlying BGN-type encryption system based on the hardness of the D-U-LWE problem. The scheme is collusion-resistant, noninteractive and anonymous. We also prove the scheme is IND-sID-CPA secure and resists quantum attack in the standard model. Because the related operations and storage only involve polynomials with small coefficients, the scheme based on the RLWE hard problem [24] can achieve faster operations and less storage overheads. Therefore, how to construct a new multibit IB-PRE scheme based on the RLWE hard problem is one direction for future research, meanwhile, extending single-bit encryption to multibit encryption is also the other direction for future research in our scheme.

Data Availability

The data used to support the findings of this study are available from the corresponding author upon request.

Conflicts of Interest

The authors declare that they have no conflicts of interest.

Acknowledgments

The authors acknowledge the financial support from the National Key Research and Development Program of China under Grant no. 2021YFB3101100; Key Program of the National Natural Science Union Foundation of China under Grant no. U1836205; Project of High-Level Innovative Talents of Guizhou Province under Grant no. [2020]6008; Science and Technology Program of Guiyang under Grant no. [2021]1–5; Science and Technology Program of Guiyang under Grant no. [2022]2–4; and Science and Technology Program of Guizhou Province under Grant nos. [2020]5017, [2022]065.

References

[1] M. Blaze, G. Bleumer, and M. Strauss, "Divertible protocols and atomic proxy cryptography," in *Advances in Cryptology — EUROCRYPT'98, LNCS*, K. Nyberg, Ed., Springer, Berlin, Heidelberg, 1998.

[2] P. Xu, T. F. Jiao, Q. H. Wu, W. Wang, and H. Jin, "Conditional identity-based broadcast proxy re-encryption and its application to cloud email," *IEEE Transactions on Computers*, vol. 65, no. 1, pp. 66–79, 2016.

[3] X. A. Wang, F. Xhafa, J. F. Ma, and Z. H. Zheng, "Controlled secure social cloud data sharing based on a novel identity based proxy re-encryption plus scheme," *Journal of Parallel and Distributed Computing*, vol. 130, pp. 153–165, 2019.

[4] G. Kan, C. H. Jin, H. H. Zhu, Y. L. Xu, and N. Liu, "An identity-based proxy re-encryption for data deduplication in cloud," *Journal of Systems Architecture*, vol. 121, pp. 102332–102339, 2021.

[5] S. Pachala, C. Rupa, and L. Sumalatha, "l-PEES-IMP: lightweight proxy re-encryption-based identity management protocol for enhancing privacy over multi-cloud environment," *Automated Software Engineering*, vol. 29, no. 4, pp. 1–21, 2022.

[6] P. W. Shor, "Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer," *SIAM Journal on Computing*, vol. 26, no. 5, pp. 1484–1509, 1997.

[7] K. Xagawa, *Cryptography with lattices*, PhD Thesis, Department of Mathematical and Computing Sciences Tokyo Institute of Technology, Tokyo, Japan, 2010.

[8] Y. Aono, X. Boyen, L. T. Phong, and L. H. Wang, "Key-private proxy re-encryption under LWE," in *Progress in Cryptology – INDOCRYPT 2013, LNCS*, G. Paul and S. Vaudenay, Eds., pp. 1–18, Springer, Berlin, Heidelberg, 2013.

[9] K. Singh, C. P. Rangan, and A. K. Banerjee, "Lattice based identity based proxy re-encryption scheme," *Journal of Internet Services and Information Security*, vol. 3, no. 3/4, pp. 38–51, 2013.

[10] K. Singh, C. P. Rangan, and A. K. Banerjee, "Cryptanalysis of unidirectional proxy re-encryption scheme," in *Information and Communication Technology - EurAsia Conference 2014, LNCS*, M. S. Linawati, E. J. Mahendra, A. M. Neuhold, and I. Tjoa, Eds., pp. 564–575, Springer, Berlin, Heidelberg, 2014.

[11] K. Singh, C. P. Rangan, and A. K. Banerjee, "Cryptanalysis of unidirectional proxy re-encryption scheme," in *Security, Privacy, and Applied Cryptography Engineering*, R. S. Chakraborty, V. Matyas, and P. Schaumont, Eds., pp. 76–91, Springer, Berlin, Heidelberg, 2014.

[12] D. Micciancio and C. Peikert, "Trapdoors for lattices: simpler, tighter, faster, smaller," in *Advances in Cryptology – EUROCRYPT 2012 , LNCS*, D. Pointcheval and T. Johansson, Eds., pp. 700–718, Springer, Berlin, Heidelberg, 2012.

[13] L. Q. Wu, X. Y. Yang, M. Q. Zhang, and X. A. Wang, "Lattice-based multi-use unidirectional proxy re-encryption," *Journal of Huazhong University of Science and Technology*, vol. 44, no. 3, pp. 110–115, 2016.

[14] M. M. Jiang, Y. P. Hu, B. C. Wang, F. H. Wang, and Q. Q. Lai, "Lattice-based multi-use unidirectional proxy re-encryption," *Security and Communication Networks*, vol. 8, no. 18, pp. 3796–3803, 2015.

[15] C. Gentry, S. Halevi, and V. Vaikuntanathan, "A simple BGN-type cryptosystem from LWE," in *Advances in Cryptology – EUROCRYPT 2010, LNCS*, H. Gilbert, Ed., pp. 506–522, Springer, Berlin, Heidelberg, 2010.

[16] X. Y. Wang, A. Q. Hu, and H. Fang, "Improved collusion-resistant unidirectional proxy re-encryption scheme from lattice," *IET Information Security*, vol. 14, no. 3, pp. 342–351, 2020.

[17] J. Q. Hou, M. M. Jiang, Y. Y. Guo, and W. G. Song, "Efficient identity-based multi-bit proxy re-encryption over lattice in the standard model," *Journal of Information Security and Applications*, vol. 47, pp. 329–334, 2019.

[18] C. Gentry, C. Peikert, and V. Vaikuntanathan, "Trapdoors for hard lattices and new cryptographic constructions," in

Proceedings of the fortieth annual ACM symposium on Theory of computing: STOC '08, pp. 197–206, ACM, Victoria British Columbia Canada, May 2008.

[19] D. Cash, D. Hofheinz, E. Kiltz, and C. Peikert, "Bonsai trees, or how to delegate a lattice basis," *Journal of Cryptology*, vol. 25, no. 4, pp. 601–639, 2012.

[20] O. Regev, "On lattices, learning with errors, random linear codes, and cryptography," in *Proceedings of the thirty-seventh annual ACM symposium on Theory of computing: STOC '05*, pp. 84–93, ACM, New York NY USA, January 2005.

[21] N. Döttling and J. Müller-Quade, "Lossy codes and a new variant of the learning-with-errors problem," in *Advances in Cryptology – EUROCRYPT 2013, LNCS*, T. SJohansson and P. Q. Nguyen, Eds., pp. 18–34, Springer, Berlin, Heidelberg, 2013.

[22] S. Agrawal, D. Boneh, and X. Boyen, "Efficient lattice (H)IBE in the standard model," in *Advances in Cryptology–EUROCRYPT 2010 , LNCS*, H. Gilbert, Ed., pp. 553–572, Springer, Berlin, Heidelberg, 2010.

[23] M. Green and G. Ateniese, "Identity-based proxy Re-encryption," in *Applied Cryptography and Network Security. ACNS 2007, LNCS*, J. Katz and M. Yung, Eds., Springer, Berlin, Heidelberg, 2007.

[24] V. Lyubashevsky, C. Peikert, and O. Regev, "On ideal lattices and learning with errors over rings," in *Advances in Cryptology–EUROCRYPT 2010, LNCS*, H. Gilbert, Ed., pp. 1–23, Springer, Berlin, Heidelberg, 2010.